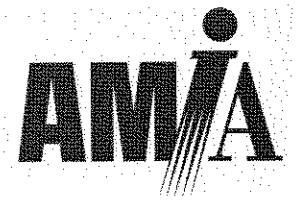

American Medical Informatics Association

4915 St. Elmo Avenue
Suite 401
Bethesda, MD 20814

Phone 301.657.1291
Fax 301.657.1296
www.amia.org

Testimony of

Don E. Detmer, MD, MA
President and Chief Executive Officer
American Medical Informatics Association

Getting to a 'Smarter' Health Information System: Legislative Proposals to Promote the Adoption of Electronic Health Records (EHRs)

Before the Committee on Energy and Commerce, Subcommittee on Health

March 16, 2006

Good morning. Chairman Deal, Ranking Member Brown, members of the Health subcommittee: thank you for the opportunity to appear before you today. My name is Don Detmer. I am President and CEO of the American Medical Informatics Association, whose 3200 members include physicians, nurses, computer and information scientists and managers, biomedical engineers, academic researchers and educators. Over the years AMIA has provided many of the thought leaders who have pioneered the innovative use of information technologies in healthcare. In addition to my role with AMIA, I am a Professor of Medical Education in the Department of Public Health Sciences at the University of Virginia. I practiced as a vascular surgeon for twenty-five years.

From 1996 to 1998 I had the privilege of serving as Chairman of the National Committee on Vital and Health Statistics, whose mission, broadly, is to advise the Department of Health and Human Services on shaping a national information strategy to improve the nation's health. My tenure at NCVHS coincided with the expansion of the Committee's charge enacted in the Health Insurance Portability and Accountability Act of 1996, which gave the Committee significant responsibilities in regard to administrative simplification and privacy. More recently, I was a member of the Commission on Systemic Interoperability, which was created by the Medicare Modernization Act, and which made a series of recommendations concerning the adoption and implementation of health information technology in an October 2005 report to Congress entitled, *Ending the Document Game: Connecting and Transforming Your Healthcare Through Information Technology*.

As you consider, and I hope pass, legislation that aims to facilitate movement toward a 'smarter' health care system through the promotion of widespread adoption of electronic health records (EHRs) and personal health records (PHRs), let me comment today on three important issues:

- first, there is a critical need for ongoing Federal leadership in encouraging and shaping a national health information system that benefits all stakeholders, especially patients;
- second, we should focus on "lessons learned" from the rollout of HIPAA standards to date and identify issues to be considered as additional health information standards and initiatives are developed and disseminated;
- and, third, we should address some current disincentives – both real and perceived – that slow the implementation of health information technologies in our healthcare system, the most information-intensive enterprise in our economy.

The Continuing Need for Federal Leadership

While it is the undoubted world leader in high technology clinical care and biomedical research, the US healthcare system is an incredibly fragmented mix of very large and very small players – a conglomeration of 21st century medical science and cottage-industry business practices, and too often characterized by uneven access, delivery and outcomes. Significant improvements in healthcare safety and quality will not be achieved for Americans without robust, secure electronic health records within a national health information infrastructure (NHII). Market forces alone have not driven the necessary integration of the interests and needs of disparate participants: hospitals – physicians and other providers – payers – employers – researchers – educators – and, most important, patients. As a result, too few individuals have access to

electronic health record systems today and there is little interconnectedness of the systems that exist. Without Federal leadership to encourage the deployment of interconnected, interoperable health information systems, our progress toward integrated and quality-based care delivery will continue to be lurching and inconsistent.

AMIA has been encouraged by Congressional attention to health information issues as evidenced by the introduction of HR 4157, the Health Information Technology Promotion Act, and HR 2234, the 21st Century Health Information Act, as well as the passage by the Senate late last year of S 1418, the Wired for Health Care Quality Act. And, we have been pleased to provide input to several legislative proposals to make personal health records (PHRs) available to Federal Employee Health Benefit Plan (FEHBP) beneficiaries. These bills are important not only for their specific provisions, some of which I will focus on today, but also because they convey an important message to the public – that their elected representatives recognize the critical importance of improving the health care system in ways that will empower consumers, while also improving the quality, safety, cost-effectiveness and accessibility of healthcare.

Over the last two plus years, the Office of the National Coordinator for Health Information Technology (ONC), which is headed by Dr. David Brailer, a Fellow of AMIA's College of Medical Informatics, has done an excellent job in communicating a vision to support widespread adoption of interoperable electronic health records within the next 10 years. AMIA is pleased that among the projects currently funded by the ONC are contracts for an Internet-based national health information network and for the development of processes for the harmonization of the various health information standards that are emerging. AMIA itself has a contract with the ONC to create a plan for a national framework for clinical decision support. In regard to interoperability standards and the development of processes to certify health information technologies that can actually 'talk' to each other and will allow the seamless integration of information systems to facilitate quality care, AMIA is also very supportive of the work of the public-private American Health Information Community (AHIC).

We believe strongly that HHS should be given explicit responsibility for ensuring the ongoing maintenance and dissemination of health information standards, with authorization for licensing and/or other types of support. To give you a successful example of Federal leadership, I would point to Secretary Tommy Thompson's drive to complete the licensure and distribution of SNOMED-CT, a vital 'dictionary' of medical terminology, by the National Library of Medicine in 2004. AMIA firmly believes that the Department should draw heavily on the resources and expertise of the NLM, and we support additional funding for the Library to ensure that approved vocabulary and other data content standards are maintained, coordinated and updated regularly to permit appropriate alignment and uniformity of the sets of standards that underlie genuinely workable EHRs and PHRs. Just like the NLM's PubMed, these standards should be openly available on the internet.

Importantly, HR 4157, the Health Information Technology Promotion Act, introduced by Chairman Deal and Representative Nancy Johnson, provides explicit and reasonable rulemaking procedures by which HHS can undertake long overdue upgrades to data vocabularies and classification systems. Simply, if we are going to facilitate development of an interoperative nationwide network of electronic health records (EHRs), we must address the issue of

interoperative data. This means that we must have standard vocabularies as the source of our primary data in the electronic health record, and use contemporary disease classifications and coding systems, (ICD-10), not only for traditional reimbursement purposes but to permit meaningful and accurate secondary uses of data for quality, biosurveillance, and public health monitoring, health research, injury prevention and policy making. As a physician and a health informatician, I find it unacceptable that the US remains one of a true handful of countries in the world to use a 30-year old classification system for diagnoses and inpatient procedures. If we are serious about deploying electronic health record systems for the benefit of individual patients and the nation as a whole, we must attend to the need to improve data standards and speed our capacity to update those standards. At the end of the day, our data systems and standards should primarily foster better care, not better reimbursement.

HR 4157 establishes the Office of the National Coordinator for Health Information Technology in statute, and I believe this step is a crucial one in clarifying Federal leadership. As part of our support for the Office of the National Coordinator, AMIA will continue to urge the appropriators on both sides of the Hill to provide for adequate funding of the ONC.

Examining HIPAA Lessons Learned So Far

As we move to develop an interconnected, interoperable health information system that will facilitate quality, access and patient-centeredness on a national and international basis, it is prudent to identify lessons we have learned so far from the administrative simplification provisions of HIPAA. Though the road was often difficult, if not actually painful, we have made a great deal of progress in establishing the rights of individuals to expect that their health information will be used appropriately and their privacy and confidentiality protected, and in imposing meaningful and reasonable obligations on health care providers, plans and payers, and others to comply with consistent Federal standards for the use, disclosure and transmission of health information.

Where once some people in the healthcare system may have treated individual health information too cavalierly on at least some occasions, from my perspective it is manifestly clear that since the Privacy Rule took effect in 2003, doctors, hospitals, pharmacies, health plans and others have made really extraordinary efforts to inform individuals of their rights and to establish policies and procedures that protect sensitive health information. Today every individual has a Federal right to access his or her medical record and to expect that the healthcare system will keep that record secure and confidential. And these norms are national – no longer are your rights, or the legal responsibilities of those healthcare providers you deal with, defined by the unique features of the State in which you live. Even if HIPAA may have 'backed' the nation into reasonable privacy and confidentiality protections, the roll-out has proved, on the whole, successful.

Notwithstanding what I think have been extremely good faith efforts to ensure that personal data is adequately protected, I do not discount that some people – for instance, those with concerns about the security of especially sensitive information, such as HIV status or relating to mental health treatment – have continued concerns about health privacy. To my knowledge there have not been reports of any large-scale violations of the framework set in place by the HIPAA

Privacy Rule. That is, individually identifiable health information is used and disclosed only for "treatment, payment and health care operations" or as otherwise specifically authorized by the individual. Does the Privacy Rule protect against patently unethical or extraordinarily careless acts – like the leaking of a celebrity's medical record to a tabloid magazine or the disposal of old medical records in a dumpster or a straightforward instance of identity theft? Of course not – but we cannot expect even the most carefully crafted information standards to prevent all illegal behavior. In such instances, active pursuit and strong penalties are needed when intrusions and misuses are identified, as a lesson to dissuade others from similar illegal behavior.

Some argue that the States must have the capacity to enact 'more stringent' standards for health information – as is true under the current Privacy Rule – for all health information standards, including those that are absolutely necessary for the development of an interconnected, interoperable national health information system. In the name of better healthcare, I must respectfully disagree. About half of all Americans live near State lines and multiple State approaches complicate the efficient and seamless transmission of crucial health information. For example, it is hardly unusual for an individual to work in the District, live in Maryland, and receive health care in Virginia, with payments made by an insurer located in still another state. If we are to ensure real-time availability of accurate and complete clinical information at the point of care, we simply cannot have the standards for the use, disclosure and transmission of the patient's health information subject to idiosyncratic requirements of individual States.

Personally, I don't see how we can get to the common standards and interoperability that underlie the widespread adoption of electronic health records without Federal preemption of conflicting State laws. But rather than simply assert that proposition, let me note that, in relation to the Privacy Rule, since 1999 AMIA has called for a study of the impact of the lack of Federal preemption and the impact of varying State statutes on the rights and protections afforded to individuals and upon the quality, cost and effectiveness of health care. Thus, I am very pleased that HR 4157 calls upon the Secretary to undertake such a study in relation to standards that have been adopted subsequent to HIPAA. This is a prudent approach; however, if the study shows that varying State laws and requirements have a negative impact on health care delivery, quality and access, and that HIPAA has established meaningful privacy and security protections, it makes sense to move forward without delay on Federal preemption for all adopted HIPAA standards.

As you may recall, the original HIPAA legislation called for the development of a unique personal healthcare identifier for individuals. All other developed economies in the world have already or are currently implementing such identifiers to assure proper authentication of people seeking care services. Whether we do so with via a voluntary opt-out approach or through the use of reliable identification algorithms, the United States needs a uniform approach to authenticating one's identity, and having the benefit of a unique identifier to help increase the ease and accuracy of this authentication is not trivial. Indeed, I fear that short of such a move, we will be left behind the other nations with whom we should be seeking secure ways to collaborate on global standards. This topic was a key recommendation from the Commission on Systemic Interoperability, and I would strongly recommend that consideration of the issues involved in the reliable authentication of individuals be included in the Secretarial study called for in HR 4157.

Disincentives That Have Slowed Implementation of Information Technologies

From 1999 through 2003 I had the privilege to serve as the Gillings Professor of Health Management at Cambridge University in England and to consult to the National IT programme of the National Health Service. As you may know, the British government is investing billions of pounds to implement a fully functional, patient-friendly, electronic health record and system. While this task might appear to be easier in some aspects because of Britain's single-payer system, of particular note to me was the observation that, even before the government's new investment, well over 80 percent of England's primary care physicians were facilitating patient care electronically. Today they are moving forward with booking appointments, writing prescriptions, making electronic referrals, recording clinical notes and tracking treatment compliance. By contrast, it is estimated that fewer than 20 percent of US primary care physicians utilize electronic health records.

Interestingly, England's primary care practices were 'wired' initially not because of government investment, but because the British pharmaceutical industry years ago offered to supply the necessary hardware and software to primary care doctors in return for access to anonymized prescribing information. In the United States I think such an arrangement would be seen as unseemly at best, and illegal at worst; certainly in the U.K. there were those who held the same view. While the British are neither less ethical nor more permissive of the misuse of identifiable health information than are Americans, in this country hospitals, physicians and other providers are incredibly reluctant to pursue any innovative financing for health IT, including networks that can securely link together a region's providers, because of their concerns about the Stark self-referral prohibitions and other fraud and abuse standards.

Whether these concerns are reasonable, today we have hospital lawyers who absolutely insist that it is simply not acceptable for any third party to furnish any information technologies – whether hardware, software, training or other services – to any provider at less than a full, fair market price. Yet, the aims of HIT dissemination are to improve the availability of accurate and timely health information in order to improve the quality of care, and I am aware of no evidence that such dissemination by a hospital, for instance, could actually serve to drive 'new' referrals or business into that hospital. While some healthcare systems and providers are moving forward under the current standards, the general consensus in the healthcare community is that the Stark provisions, while quite important in many respects, are significantly constraining progress on the roll-out of electronic health record systems.

It is in the interest of all stakeholders, particularly patients, that functional electronic health records and an interoperable health information system be deployed as promptly as possible. But the entities that are one key to making crucial progress with that deployment, the small and rural physician practices that still provide a majority of health care services in this country, are those that are least able to afford the capital investment for the purchase and hassle of implementing state-of-the art IT systems. Especially because most of the 'savings' of health IT accrue to other system participants, including employers, health plans and patients, financial outlays necessary for the purchase of the very building blocks of an NHII should reasonably come from a wide

variety of sources, including government outlays and pay-for-performance programs. Actually, pay-for-performance programs represent a clear argument for payers to provide some of the financing for health IT – because in order to pay for performance you have to be able to track performance and quality in the delivery of care, and to do that efficiently you need sophisticated information capabilities embedded in the healthcare system. Reasonable safe harbors for dissemination of health information technologies and services intended to improve healthcare quality, efficiency and access would encourage deployment of essential health information systems, and I am very pleased that provisions to that effect are included in Chairman Deal's bill.

Educating the Healthcare Workforce

There is no question that momentum for bringing healthcare into the information century is building, but this won't happen purely through a widespread distribution of hardware and software and standards and certifications. Ultimately, IT comes down to healthcare workers and patients being sufficiently skilled to take real advantage of the opportunities for improved care and efficiency and access that health information technologies and an interconnected national health information infrastructure can provide. Assuring these skills throughout the workforce will necessitate sufficient numbers of well educated health informaticians. Because the field is advancing so rapidly, we are seriously undersupplied to meet this challenge.

Last year to help address this challenge, AMIA announced its 10 by 10 program, which aims to realize a goal of training 10,000 health care professionals, especially in applied clinical informatics by the year 2010; we just passed our first 100 graduates of a largely web-based course developed by William Hersh and his colleagues at the Oregon Health and Science University. Other universities intend to participate as well. Our program uses classes, tutorials, web-based and in-person sessions to equip health care professionals to use health information and health information technologies to benefit patient care and to advance medical knowledge. In fact, we know from the research of AMIA members that well-trained health providers combined with robust IT systems can produce safer, higher quality care delivery.

With the supply of physicians essentially constant and the nursing workforce aging along with the baby boomers, we will only be able to address the increasing demands for care of a growing and aging population by developing a better trained workforce, especially more nurses skilled in the use of information and information systems. Increased Federal support for education and training will be needed to address this workforce reality – and in November 2005 AMIA, in conjunction with our colleagues of the American Health Information Management Association (AHIMA), convened a workforce summit, which included broad representation of stakeholders across the healthcare enterprise, to develop initial strategies to address challenges related to effective implementation of EHRs and PHRs. The resulting white paper, *Building the Workforce for Health Information Transformation* presents nine targeted recommendations that the industry – including employers, employees, vendors, the government and professional organizations – can use to prepare the existing workforce to use technology tools and to ensure that we have a sufficient number of well-qualified health information specialists to achieve the promise of health IT transformation.

A Few Conclusions

In terms of the development and implementation of integrated health information systems with sophisticated capabilities, we have seen a great deal of progress in the last few years. Within the Veteran's Administration, for instance, the case for improved safety and higher quality through the proper use of IT systems – including electronic records, decision-support programs, and process tracking and change analyses – has been largely made. We have seen the creation of the Office of the National Coordinator for Information Technology and a Commission to Certify Health Information Technology. The Commission on Systemic Interoperability mandated by the MMA has provided an important set of recommendations to Congress, and Secretary Leavitt has pressed the American Health Information Community (AHIC) to take on a range of public-private initiatives to develop information standards, certify new technologies, and provide long-term planning and governance for the electronic health environment.

Someday we may look back at this moment and say, "The rest is history" – but not just yet. Additional legislation and Federal support, and the development of accepted, enterprise-wide standards will be required if true interoperability and connectedness are to occur. Clearly, HR 4157 does not try to address all of the issues involved in creating an NHII to improve healthcare quality, access and patient-centeredness. But it does forthrightly address some key 'sticking points' that are keeping the nation from moving forward as quickly as we should and among them are first, establishment of the Office of the National Coordinator in statute; second, addressing the impact on patient's rights and on healthcare quality and safety of varying and conflicting State and Federal information standards; and, third, reducing some current disincentives to the adoption of available health information technologies. AMIA looks forward to prompt consideration of the legislation and to supporting its implementation.

Finally, let's not forget that an interoperable, interconnected national information system is not only a healthcare issue; it is a matter of national security. When I testified to the House Ways and Means Committee on July 25, 2005, I stated that it wasn't clear what would bring this reality to the American public. I mentioned an outbreak of avian flu in a US population center or an episode of bioterrorism or the occurrence of transmissible disease in our food supply chain. Instead, a few months later Hurricane Katrina drove home my point. In the first weeks and months after this national disaster, two contrasting points were made abundantly clear. First, public health and individual patient care of thousands of Americans was jeopardized as paper medical records were destroyed by mud. Second, the electronic medication and health records of veterans were available wherever and whenever their availability was authorized, offering immediate help to hundreds. People's lives do hang in this balance.

We must have a reliable, ubiquitous electronic health information system for our nation. It is crucial for personal health, public health and the economic interests of our country. While widespread dissemination of electronic health record systems and the development of a functional NHII will facilitate broad improvements in health care quality, access and affordability, it will also assist in protecting our security and I would urge your leadership in facilitating this development with all due speed.

Thank you for the opportunity to appear before you today. I will be happy to answer any questions.